

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-268946

(43)Date of publication of application : 20.09.2002

(51)Int.Cl. G06F 12/14

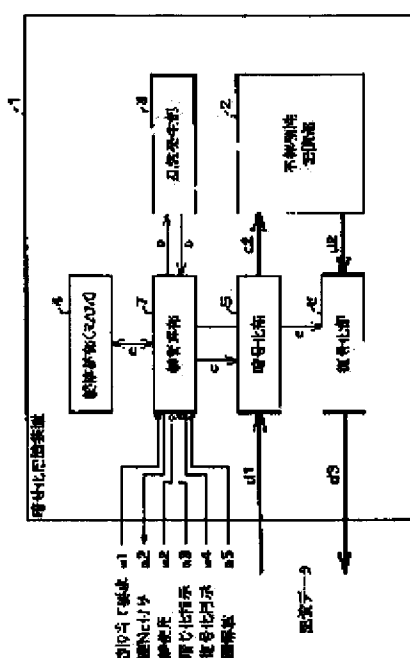
G11B 20/10

G11B 27/00

(21)Application number : 2001-067700 (71)Applicant : SHARP CORP

(22)Date of filing : 09.03.2001 (72)Inventor : OBARA RYOKO
HAMADA AKIRA

(54) DATA STORAGE DEVICE



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data storage device capable of suppressing chain discrimination of stored data of a nonvolatile storage device by persons not concerned.

SOLUTION: In an encryption storage device 1, a key managing part 7 outputs a generation request signal b to a random number generating part 3 when an allocation request signal a1 is inputted. The random number generating part 3 generates a pseudo random number at input timing of the generation request signal b, adopts it as an encryption key, the key managing part 7 stores the encryption key c into a volatile key storage part 4 and returns a corresponding key number a2 to the user side. When the user inputs an encryption instruction signal a3 and the key number a2 to the key managing part 7, the key managing part 7 reads a corresponding encryption key c, an encrypting part 5 converts data d1 to be

inputted into encrypted data d2 and stores it in a nonvolatile storage part 2. When the user inputs a decryption instruction signal a4 and the key number a2 to the key managing part 7, the key managing part 7 reads the corresponding key number c and a decrypting part 6 converts the encrypted data into decrypted data d3.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-268946
(P2002-268946A)

(43)公開日 平成14年9月20日(2002.9.20)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/14	3 2 0	C 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 1 1 B 20/10		C 1 1 B 20/10	H 5 D 0 4 4
27/00		27/00	D 5 D 1 1 0

審査請求 未請求 請求項の数9 O L (全 14 頁)

(21)出願番号 特願2001-67700(P2001-67700)

(22)出願日 平成13年3月9日(2001.3.9)

(71)出願人 000003049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72)発明者 小原 良子

大阪府大阪市阿倍野区長池町22番22号 シ
ャープ株式会社内

(72)発明者 濱田 明

大阪府大阪市阿倍野区長池町22番22号 シ
ャープ株式会社内

(74)代理人 100080034

弁理士 原 謙三

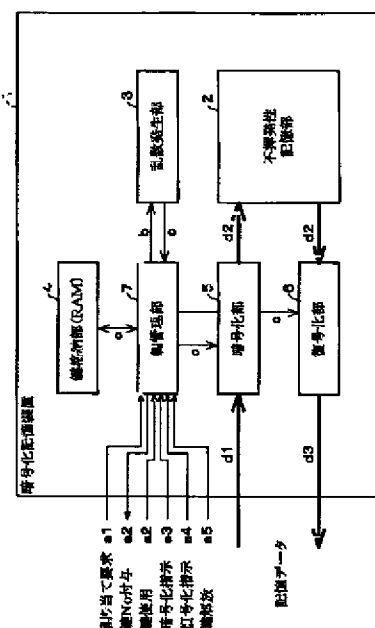
最終頁に続く

(54)【発明の名称】 データ記憶装置

(57)【要約】

【課題】 非関係者に不揮発性の記憶装置の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供する。

【解決手段】 暗号化記憶装置1において、鍵管理部7は割り当て要求信号a1が入力されると乱数発生部3に生成要求信号bを出力する。乱数発生部3は生成要求信号bの入力タイミングで擬似乱数を生成してこれを暗号鍵cとし、鍵管理部7は該暗号鍵cを揮発性の鍵格納部4に記憶させるとともに、対応する鍵番号a2を使用者側へ返す。使用者が暗号化指示信号a3と鍵番号a2とを鍵管理部7に入力すると、鍵管理部7は対応する暗号鍵cを読み出し、暗号化部5が入力されるデータd1を暗号化データd2に変換して不揮発性記憶部2に記憶させる。使用者が復号化指示信号a4と鍵番号a2とを鍵管理部7に入力すると、鍵管理部7は対応する暗号鍵cを読み出し、復号化部6が暗号化データd2を復号データd3に変換する。



【特許請求の範囲】

【請求項1】データを記憶する記憶データ不揮発性の不揮発性記憶手段を備えたデータ記憶装置において、所定のタイミングで擬似乱数を生成し、上記タイミングごとの擬似乱数を暗号鍵とする暗号鍵発生手段と、上記暗号鍵発生手段によって生成された上記暗号鍵を記憶する記憶データ揮発性の暗号鍵記憶手段と、上記暗号鍵が与えられると、入力されるデータを上記暗号鍵によって暗号化して上記不揮発性記憶手段に暗号化データとして記憶させる暗号化手段と、暗号化の際と同一の上記暗号鍵が与えられると、上記不揮発性記憶手段に記憶されている上記暗号化データを上記暗号鍵によって復号化して読み出す復号化手段と、外部から行われる使用者への上記暗号鍵の割り当て要求に対して上記割り当て要求時に最新の上記暗号鍵に対応する暗号鍵情報を返し、入力されるデータを暗号化する指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記暗号化手段に与え、上記暗号化データを読み出す指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記復号化手段に与える暗号鍵管理手段と、を備えていることを特徴とするデータ記憶装置。

【請求項2】上記暗号鍵発生手段は、外部からの上記暗号鍵の生成要求を受け付け、上記生成要求時を上記所定のタイミングとして上記暗号鍵を生成することを特徴とする請求項1に記載のデータ記憶装置。

【請求項3】上記暗号鍵管理手段は、上記割り当て要求時に上記暗号鍵発生手段に上記生成要求を行うことを特徴とする請求項2に記載のデータ記憶装置。

【請求項4】一定時間ごとに信号を生成するタイマーを備え、上記暗号鍵発生手段の上記所定のタイミングが上記信号の生成タイミングに連動していることを特徴とする請求項1ないし3のいずれかに記載のデータ記憶装置。

【請求項5】上記暗号鍵記憶手段に複数の上記暗号鍵が記憶されることを特徴とする請求項1ないし4のいずれかに記載のデータ記憶装置。

【請求項6】上記暗号鍵管理手段は、上記暗号鍵発生手段によって生成された最新の上記暗号鍵を上記暗号鍵記憶手段に既に記憶されている上記暗号鍵と比較して一致するものがある場合には、上記暗号鍵発生手段に最新の上記暗号鍵を一致しなくなるまで生成し直させ、一致する上記暗号鍵は使用者に割り当てないことを特徴とする請求項1ないし5のいずれかに記載のデータ記憶装置。

【請求項7】上記暗号鍵管理手段は、外部から上記暗号鍵を無効にする指示を上記暗号鍵に対応する上記暗号鍵情報との組合せで受け付けて、上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないようにすることを特徴とする請求項1ない

し6のいずれかに記載のデータ記憶装置。

【請求項8】上記暗号鍵管理手段は、上記暗号鍵の使用者への割り当てから所定時間が経過すると上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないことを特徴とする請求項1ないし7のいずれかに記載のデータ記憶装置。

【請求項9】擬似乱数を上記暗号鍵情報として生成する暗号鍵情報発生手段を備えていることを特徴とする請求項1ないし8のいずれかに記載のデータ記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データを記憶するデータ記憶装置に関するものである。

【0002】

【従来の技術】機密データを不揮発性の記憶媒体に記憶するデータ記憶装置は種々提案されている。

【0003】例えば記憶されたデータの読み出しを制限するために、特開昭62-107352号公報には、データを記憶するROMと、暗号鍵が書き込まれる揮発性メモリもしくは揮発性レジスタとを備えた暗号化ROM装置が開示されている。この暗号化ROM装置にデータを記憶させる場合には、揮発性メモリもしくは揮発性レジスタに暗号鍵を書き込み、該暗号鍵でデータを暗号化してROMに記憶する。また、暗号化ROM装置からデータを読み出す場合には、揮発性メモリもしくは揮発性レジスタに暗号鍵を書き込み、該暗号鍵でROMのデータを復号化する。揮発性メモリもしくは揮発性レジスタに書き込まれた暗号鍵は、暗号化ROM装置の電源を断にすることによって容易に消滅するので、単に電源を再投入しただけではROMのデータを読み出すことができないようになっている。

【0004】また、既に必要がなくなった機密データについて、特開平09-223061号公報には、機密データが格納されたハードディスクなどの情報の格納領域から、機密データの読み出し処理の終了後に、データの格納位置などを管理するFATなどのインデックスのみならず機密データをも消去して機密保持を強化しようとする情報処理装置が開示されている。

【0005】

【発明が解決しようとする課題】しかしながら、上記特開昭62-107352号公報の暗号化ROM装置では、ROMに解析しやすいデータが記憶されている状態で部外者に持ち出されるなどして記憶内容が解析されると、消滅した暗号鍵が推測される虞がある。非関係者に暗号鍵が知られると、この暗号化ROM装置に記憶されるデータが次々に復号化される危険性がある。この危険は、解析したROMに記憶されている他のデータのみならず、今後この暗号化ROM装置に記憶されるデータにも及ぶ。

【0006】また、特開平09-223061号公報の

情報処理装置の場合、インデックスに加えて機密データそのものを消去するため、消去すべきデータのサイズが大きい。従って、消去に要する時間が増大することになり、情報の格納領域に対するデータ入出力の効率の低下を招く虞がある。

【0007】本発明は、上記従来の問題点に鑑みなされたものであり、その目的は、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供することにある。また、本発明の他の目的は、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置を提供することにある。

【0008】

【課題を解決するための手段】本発明のデータ記憶装置は、上記課題を解決するために、データを記憶する記憶データ不揮発性の不揮発性記憶手段を備えたデータ記憶装置において、所定のタイミングで擬似乱数を生成し、上記タイミングごとの擬似乱数を暗号鍵とする暗号鍵発生手段と、上記暗号鍵発生手段によって生成された上記暗号鍵を記憶する記憶データ揮発性の暗号鍵記憶手段と、上記暗号鍵が与えられると、入力されるデータを上記暗号鍵によって暗号化して上記不揮発性記憶手段に暗号化データとして記憶させる暗号化手段と、暗号化の際と同一の上記暗号鍵が与えられると、上記不揮発性記憶手段に記憶されている上記暗号化データを上記暗号鍵によって復号化して読み出す復号化手段と、外部から行われる使用者への上記暗号鍵の割り当て要求に対して上記割り当て要求時に最新の上記暗号鍵に対応する暗号鍵情報を返し、入力されるデータを暗号化する指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記暗号化手段に与え、上記暗号化データを読み出す指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記復号化手段に与える暗号鍵管理手段と、を備えていることを特徴としている。

【0009】上記の発明によれば、暗号鍵発生手段が所定のタイミングで擬似乱数を発生して各タイミングでの擬似乱数を暗号鍵とし、暗号鍵記憶手段がこの暗号鍵を記憶する。そして、暗号鍵管理手段は、外部から使用者が暗号鍵の割り当てを要求してきたときに最新の暗号鍵に対応する暗号鍵情報を使用者に返す。使用者によってデータの暗号化の指示と暗号鍵情報とが入力されると、その暗号鍵情報に対応する暗号鍵を暗号鍵記憶手段から読み出して暗号化手段に与える。暗号化手段は入力されるデータを与えられた暗号鍵によって暗号化して不揮発性記憶手段、すなわち不揮発性の記憶媒体に暗号化データとして記憶させる。

【0010】また、暗号鍵管理手段は、使用者によって

暗号化データを読み出す指示および暗号鍵情報が入力されると、その暗号鍵情報に対応する暗号鍵を暗号鍵記憶手段から読み出して復号化手段に与える。復号化手段は、暗号化の際と同一の暗号鍵が与えられると、不揮発性記憶手段に記憶されている暗号化データを暗号鍵によって復号化して読み出す。

【0011】このように、擬似乱数を暗号鍵とするので、複数の暗号鍵を生成すると同一の暗号鍵が生じる確率は極めて小さくなる。従って、生成された最新の暗号鍵を使用者に割り当てることにより、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を高い確率で異ならせることができる。これにより、様々な暗号鍵によるデータの暗号化および復号化を容易に行うことができるようになり、不揮発性記憶手段には暗号鍵の異なる複数の暗号化データを記憶させることができる。

【0012】また、暗号鍵記憶手段は記憶データ揮発性であるので、持ち出されるなどしてデータが解析される場合には、通常電源が遮断されて暗号鍵記憶手段に記憶されていた暗号鍵は消滅する。この状態で不揮発性記憶手段に記憶されている暗号化データを解析された場合、解析が容易な暗号化データが偶然存在してこの暗号化データの暗号鍵が推測されたとしても、推測された暗号鍵では、その他の異なる暗号鍵で暗号化された暗号化データを復号化することはできない。また、持ち出された不揮発性記憶手段の暗号化データについての暗号鍵が推測されたとしても、今後この不揮発性記憶手段に記憶される暗号化データの暗号鍵には擬似乱数が使用されるので、推測されたものとは異なる確率が非常に高い。従って、暗号化データが使用者以外に連鎖的に判別されることはほとんどない。

【0013】この結果、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供することができる。

【0014】また、使用者により不揮発性記憶手段に記憶されている暗号化データの復号化が行われた後など、暗号化データをこれ以上読み出す必要がなくなった場合に、上述したように非関係者による暗号鍵の推測は、解析が容易なデータでない限り困難である。従って、不揮発性記憶手段に記憶されている暗号化データを消去するといった、データ入出力の妨げとなる時間のかかる作業は不要である。この結果、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置を提供することができる。

【0015】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵発生手段は、外部からの上記暗号鍵の生成要求を受け付け、上記生成要求時を上記所定のタイミングとして上記暗号鍵を生成することを特徴としている。

【0016】上記の発明によれば、暗号鍵を生成したいときに暗号鍵発生手段に暗号鍵を生成させるので、既に生成されて暗号鍵記憶手段に記憶されている暗号鍵とは異なる暗号鍵を容易に得ることができる。また、無駄な暗号鍵の生成を避けることができる。

【0017】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、上記割り当て要求時に上記暗号鍵発生手段に上記生成要求を行うことを特徴としている。

【0018】上記の発明によれば、暗号鍵の割り当て要求時に暗号鍵発生手段に暗号鍵を生成させるので、割り当て要求ごとに異なる暗号鍵を容易に得ることができる。従って、データを他の使用者に判別されにくいものとしたり、同一使用者の読み出し対象としていないデータが読み出されてしまうことを避けたりすることができる。また、暗号鍵の生成要求を別途行わなくてもすむ。

【0019】さらに本発明のデータ記憶装置は、上記課題を解決するために、一定時間ごとに信号を生成するタイマーを備え、上記暗号鍵発生手段の上記所定のタイミングが上記信号の生成タイミングに連動していることを特徴としている。

【0020】上記の発明によれば、放置しておいても暗号鍵発生手段に暗号鍵を次々に生成させることができるので、暗号鍵の生成のきっかけを意図的に与える必要がない。

【0021】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵記憶手段に複数の上記暗号鍵が記憶されることを特徴としている。

【0022】上記の発明によれば、暗号鍵のそれぞれを別々のデータの暗号化および復号化に用いることができるので、同じ期間に異なる使用者に異なる暗号鍵を割り当てたり、同一使用者に異なるデータの処理用に異なる暗号鍵を割り当てたりすることができる。従って、同じ期間に各データの機密保持が確保された状態での不揮発性記憶手段の使用可能回数が増加し、データの暗号化および復号化の効率を向上させることができる。

【0023】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、上記暗号鍵発生手段によって生成された最新の上記暗号鍵を上記暗号鍵記憶手段に既に記憶されている上記暗号鍵と比較して一致するものがある場合には、上記暗号鍵発生手段に最新の上記暗号鍵を一致しなくなるまで生成し直させ、一致する上記暗号鍵は使用者に割り当てないことを特徴としている。

【0024】上記の発明によれば、暗号鍵記憶手段に既に記憶されている暗号鍵とは異なる最新の暗号鍵が使用者に割り当てられるので、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を確実に異ならせることができる。

【0025】さらに本発明のデータ記憶装置は、上記課題

を解決するために、上記暗号鍵管理手段は、外部から上記暗号鍵を無効にする指示を上記暗号鍵に対応する上記暗号鍵情報との組合せで受け付けて、上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないようにすることを特徴としている。

【0026】上記の発明によれば、暗号鍵をもう使用しないときにいつでも暗号鍵をデータの暗号化や復号化に使用不可とすることができるので、データが不用意に読み出される可能性を極力小さくすることができる。

【0027】さらに本発明のデータ記憶装置は、上記課題を解決するために、上記暗号鍵管理手段は、上記暗号鍵の使用者への割り当てから所定時間が経過すると上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないことを特徴としている。

【0028】上記の発明によれば、割り当てから所定時間が経過すると暗号鍵が使用不可となるので、同じ暗号鍵が使用者に長い間占有されるのを防止することができる。また、暗号鍵を使用不可とする指示を使用者から与えなくても使用不可となるので、データが不用意に読み出される可能性を自動的に極力小さくすることができる。

【0029】さらに本発明のデータ記憶装置は、上記課題を解決するために、擬似乱数を上記暗号鍵情報として生成する暗号鍵情報発生手段を備えていることを特徴としている。

【0030】上記の発明によれば、暗号鍵情報が擬似乱数で使用者に与えられるので、過去に与えられた暗号鍵情報を使用したデータの不正な暗号化および復号化が行われるのを防止することができる。

【0031】

【発明の実施の形態】〔実施の形態1〕本発明のデータ記憶装置を具現する一実施の形態について、図1ないし図7を用いて説明すれば以下の通りである。

【0032】図1に、本実施の形態に係るデータ記憶装置としての暗号化記憶装置1の構成を示す。暗号化記憶装置1は、不揮発性記憶部2、乱数発生部3、鍵格納部4、暗号化部5、復号化部6、および鍵管理部7を備えている。

【0033】不揮発性記憶部（不揮発性記憶手段）2はハードディスクやROMなど記憶データ不揮発性の記憶媒体である。不揮発性記憶部2には暗号化されたデータである暗号化データが記憶される。乱数発生部（暗号鍵発生手段）3は所定のタイミングで擬似乱数を生成し、該タイミングごとに生成した擬似乱数を暗号鍵cとする。ここでは、乱数発生部3は後述する鍵管理部7からの暗号鍵cの生成要求を受け、該生成要求時を所定のタイミングとする。鍵格納部（暗号鍵記憶手段）4はRAMなど記憶データ揮発性の記憶媒体である。鍵格納部4

は乱数発生部3で生成された暗号鍵cを鍵管理部7による管理で記憶する。

【0034】暗号化部(暗号化手段)5は、鍵管理部7から暗号鍵cが与えられると、暗号化記憶装置1の外部から入力されるデータd1を、与えられた暗号鍵cによって暗号化して不揮発性記憶部2に暗号化データd2として記憶させる。復号化部(復号化手段)6は、鍵管理部7から暗号化の際と同一の暗号鍵cが与えられると、不揮発性記憶部2に記憶されている暗号化データd2を、与えられた暗号鍵cによって復号化して読み出し、復号データd3として暗号化記憶装置1の外部に出力する。

【0035】図2(a)・(b)に暗号化部5および復号化部6の構成例を示す。同図(a)は、EX-ORゲート8によって暗号化記憶装置1の外部から入力されるデータd1と暗号鍵cとの排他的論理和をとることによって暗号化データd2を生成する暗号化部5の構成、およびEX-ORゲート8によって不揮発性記憶部2の暗号化データd2と暗号鍵cとの排他的論理和をとることによって復号データd3を生成する復号化部6の構成である。同図(b)は同図(a)の構成に暗号鍵cをトリガーとして擬似乱数eを生成してこの擬似乱数eをEX-ORゲート8に入力する暗号鍵乱数化部9を追加したものであり、EX-ORゲート8によって上記擬似乱数eとデータd1との排他的論理和をとることによって暗号化データd2を生成する暗号化部5の構成、およびEX-ORゲート8によって上記擬似乱数eと暗号化データd2との排他的論理和をとることによって復号データd3を生成する復号化部6の構成である。暗号鍵乱数化部9は同じ暗号鍵cが入力されると常に同じ擬似乱数eを出力する。同図(b)の構成では、暗号鍵cが単純な数値列であってもこれを乱数化することによって複雑な数値列に置き換え、暗号化データd2の解析によって暗号鍵cが容易に推測されないようになっている。

【0036】鍵管理部(暗号鍵管理手段)7は、暗号鍵cの発生や受け渡し、選択を管理している。鍵管理部7は、暗号化記憶装置1の外部から暗号化記憶装置1の利用者によりコンピュータを介して暗号鍵cの割り当て要求を示す割り当て要求信号a1が入力されるようになっており、割り当て要求信号a1が入力されると乱数発生部3に暗号鍵cの生成要求を示す生成要求信号bを出力する。そして乱数発生部3で生成された暗号鍵cを鍵格納部4に記憶させるとともに、生成したばかりの暗号鍵c、すなわち最新の暗号鍵cに対応する鍵番号(暗号鍵情報)a2を使用者側(コンピュータ)へ返す。鍵格納部4には乱数発生部3により過去に生成された暗号鍵cがいくつか記憶されているが、鍵番号a2は暗号鍵cごとに異なっている。

【0037】また、鍵管理部7には、暗号化の指示を示す暗号化指示信号a3と、復号化の指示を示す復号化指

示信号a4とが入力されるようになっている。使用者はデータd1を暗号化して不揮発性記憶部2に記憶させようとするとき、暗号化指示信号a3と鍵番号a2とをコンピュータを介して鍵管理部7に入力する。鍵管理部7はこの入力に基づいて鍵番号a2に対応する暗号鍵cを鍵格納部4から読み出して暗号化部5に与える。また、使用者は不揮発性記憶部2の暗号化データd2を復号化して復号データd3を読み出そうとするとき、復号化指示信号a4と鍵番号a2とをコンピュータを介して鍵管理部7に入力する。鍵管理部7はこの入力に基づいて鍵番号a2に対応する暗号鍵cを鍵格納部4から読み出して復号化部6に与える。また、鍵管理部7には、使用者が割り当てられた暗号鍵cを無効にする指示を示す鍵解放信号a5が入力されるようになっており、鍵管理部7は、鍵解放信号a5に加えてその暗号鍵cに対応する適正な鍵番号a2が入力されると、以後、その鍵番号a2が入力されても対応する暗号鍵cを暗号化部5および復号化部6に与えないようになっている。

【0038】さらに、鍵管理部7は暗号鍵cの使用者への割り当て内容を表す割り当て枠を認識して、鍵格納部4に記憶させている。図3に割り当て枠の構造の一例を示す。割り当て枠は0からNのN+1個の複数の鍵番号a2のそれぞれに対応して設けられており、割り当て枠ごとに1つの暗号鍵cが対応している。なお、割り当て枠を1つとすることも可能である。そして、暗号鍵cが割り当て枠の総数であるN+1個を上限として鍵格納部4に格納されるようになっている。鍵管理部7は、既に使用者に割り当て、現在有効である暗号鍵cの割り当て枠に使用中フラグ“1”を立てる。また、鍵管理部7は、既に使用者に割り当てたが現在無効としている暗号鍵cの割り当て枠、およびまだ使用者に暗号鍵cを割り当てていない割り当て枠に、未使用の割り当て枠であることを示すフラグ“0”を立てる。さらに、鍵管理部7は、使用中フラグ“1”を立てた割り当て枠に対して前述の鍵解放信号a5に基づいた暗号鍵cの無効化を行うと、その割り当て枠のフラグを“0”に変更する。

【0039】上記図3の割り当て枠が設けられている状態での暗号鍵cの割り当て(「鍵付与」と称する)の手順を図4のフローチャートを用いて説明する。まず、割り当て要求信号a1が鍵管理部7に入力されると、S1で鍵管理部7は未使用の割り当て枠を検索する。S2で未使用の割り当て枠が存在する場合にはS3へ進み、存在しない場合にはS8へ進んでエラー通知を使用者側(コンピュータ)へ返して処理を終了する。S3では鍵管理部7が乱数発生部3に生成要求信号bを出力して乱数発生部3に暗号鍵cを生成させる。

【0040】次いでS4で鍵管理部7は、乱数発生部3によって生成された最新の暗号鍵cとしての擬似乱数の値を、鍵格納部4に既に記憶されている暗号鍵cとしての擬似乱数の値と比較する。このとき無効とされている

暗号鍵cも比較対象とする。そして、鍵格納部4に既に記憶されている暗号鍵cの中に最新の暗号鍵cと一致するものがなければS5へ進み、一致するものがあればS3に戻って乱数発生部3に暗号鍵cを生成し直させる。従って、鍵管理部7は鍵格納部4に既に記憶されている暗号鍵cの中に最新の暗号鍵cと一致するものがなくなるまで乱数発生部3に最新の暗号鍵cを生成し直させる。一致した最新の暗号鍵cは鍵格納部4には記憶せず、自動的に使用者への割り当て対象外とする。

【0041】S5では鍵管理部7が最新の暗号鍵cを設定し、鍵格納部4に記憶させる。そして、S6で最新の暗号鍵cを未使用の割り当て枠のいずれかの暗号鍵cとし、その割り当て枠のフラグを“0”から“1”に変更する。S7でその暗号鍵cに対応する鍵番号a2を使用者に返して処理が終了する。以上が鍵付与の手順である。

【0042】次に、前記図3の割り当て枠が設けられている状態での暗号鍵cの無効化（「鍵解放」と称する）の手順を図5のフローチャートを用いて説明する。まず、鍵解放信号a5と解放しようとする暗号鍵cに対応する適正な鍵番号a2とが鍵管理部7に入力されると、S11で鍵管理部7は上記鍵番号a2の割り当て枠を検索する。そしてS12で鍵管理部7は検索した割り当て枠のフラグを“1”から“0”に変更（リセット）する。以上が鍵解放の手順である。

【0043】このように、本実施の形態の暗号化記憶装置1によれば、擬似乱数を暗号鍵cとするので、複数の暗号鍵c…を生成すると同一の暗号鍵cが生じる確率は極めて小さくなる。従って、生成された最新の暗号鍵cを使用者に割り当てることにより、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵c…を高い確率で異ならせることができる。これにより、様々な暗号鍵c…によるデータの暗号化および復号化を容易に行うことができるようになり、不揮発性記憶部2には暗号鍵cの異なる複数の暗号化データd2を記憶させることができる。

【0044】特に暗号化記憶装置1では、鍵管理部7が、乱数発生部3によって生成された最新の暗号鍵cを鍵格納部4に既に記憶されている暗号鍵c（あるいはc…）と比較して一致するものがある場合には、乱数発生部3に最新の暗号鍵cを一致しなくなるまで生成し直させ、一致する暗号鍵cは使用者に割り当てないようになっている。従って、鍵格納部4に既に記憶されている暗号鍵c（あるいはc…）とは異なる最新の暗号鍵cが使用者に割り当てられるので、鍵管理部7が割り当て要求信号a1が入力されたときに生成要求信号bを出力して乱数発生部3に新たな暗号鍵cを生成させる場合のように、擬似乱数の異なる生成タイミングを経て生成された複数の暗号鍵c…を使用者に割り当てることにより、暗号鍵c…のそれぞれを互いに確実に異ならせることがで

きる。

【0045】また、鍵格納部4は記憶データ揮発性であるので、暗号化記憶装置1が持ち出されるなどしてデータが解析される場合には、通常電源が遮断されて鍵格納部4に記憶されていた暗号鍵c（あるいはc…）は消滅する。この状態で不揮発性記憶部2に記憶されている暗号化データd2を解析された場合、解析が容易な暗号化データd2が偶然存在してこの暗号化データd2の暗号鍵cが推測されたとしても、推測された暗号鍵cでは、その他の異なる暗号鍵cで暗号化された暗号化データd2を復号化することはできない。また、持ち出された不揮発性記憶部2の暗号化データd2についての暗号鍵cが推測されたとしても、今後この不揮発性記憶部2に記憶される暗号化データd2の暗号鍵cには擬似乱数が使用されるので、推測されたものとは異なる確率が非常に高い。従って、暗号化データd2が使用者以外に連鎖的に判別されることはほとんどない。

【0046】この結果、暗号化記憶装置1は、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置となる。

【0047】また、使用者により不揮発性記憶部2に記憶されている暗号化データd2の復号化が行われた後など、暗号化データd2をこれ以上読み出す必要がなくなった場合に、上述したように非関係者による暗号鍵cの推測は、解析が容易なデータでない限り困難である。従って、不揮発性記憶部2に記憶されている暗号化データd2を消去するといった、データ入出力の妨げとなる時間のかかる作業は不要である。この結果、暗号化記憶装置1は、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置となる。

【0048】また、暗号化記憶装置1によれば、乱数発生部3は、外部からの暗号鍵cの生成要求がそのまま反映される生成要求信号bを鍵管理部7から受け付け、生成要求時を所定のタイミングとして暗号鍵cを生成する。このように、暗号鍵cを生成したいときに乱数発生部3に暗号鍵cを生成させるので、既に生成されて鍵格納部4に記憶されている暗号鍵c（あるいはc…）とは異なる暗号鍵cを容易に得ることができる。また、使用されないような無駄な暗号鍵cの生成を避けることができる。

【0049】また、暗号化記憶装置1によれば、鍵管理部7が、割り当て要求信号a1が入力されたときに乱数発生部3に生成要求信号bを出力して上記の生成要求を行っている。このように、暗号鍵cの割り当て要求時に乱数発生部3に暗号鍵cを生成させるので、割り当て要求ごとに異なる暗号鍵cを容易に得ることができる。従って、データを他の使用者に判別されにくいものとしたり、同一使用者の読み出し対象としていないデータが読

み出されてしまうことを避けたりすることができる。また、暗号鍵cの生成要求を別途行わなくてもすむ。

【0050】また、暗号化記憶装置1によれば、鍵格納部4に複数の暗号鍵c…が記憶される。従って、暗号鍵c…のそれぞれを別々のデータの暗号化および復号化に用いることができるので、同じ期間に異なる使用者に異なる暗号鍵cを割り当てたり、同一使用者に異なるデータの処理用に互いに異なる暗号鍵cを割り当てたりすることができる。従って、同じ期間に各データの機密保持が確保された状態での不揮発性記憶部2の使用可能回数が増加し、データの暗号化および復号化の効率を向上させることができる。

【0051】また、暗号化記憶装置1では、鍵管理部7が、鍵解放信号a5のように外部から暗号鍵cを無効にする指示を該暗号鍵cに対応する鍵番号a2との組合せで受け付けて、鍵番号a2が入力されても上記暗号鍵cを暗号化部5および復号化部6に与えないようになっている。従って、暗号鍵cをもう使用しないときにいつでも暗号鍵cをデータの暗号化や復号化に使用不可とすることができるので、データが不用意に読み出される可能性を極力小さくすることができる。

【0052】また、暗号化記憶装置1では、使用者に割り当てる鍵番号a2を擬似乱数としてもよい。例えば、暗号化記憶装置1で乱数発生部3を、擬似乱数を鍵番号a2として生成する暗号鍵情報発生手段としても機能させることができる。鍵番号a2を擬似乱数とした場合の割り当て枠の構造の一例を図6に示す。鍵番号a2が擬似乱数であるので、割り当て枠そのものに0からNまでの番号が付与されている。このようにすれば、鍵番号a2が擬似乱数で使用者に与えられるので、過去に与えられた鍵番号a2が現在も使用されているのではないかと推測されて過去の鍵番号a2を使用したデータの不正な暗号化および復号化が行われるのを、防止することができる。

【0053】鍵番号a2を擬似乱数とする場合の暗号鍵cの割り当て（「鍵付与」と称する）の手順を図7のフローチャートを用いて説明する。まず、割り当て要求信号a1が鍵管理部7に入力されると、S21で鍵管理部7は未使用の割り当て枠を検索する。S22で未使用の割り当て枠が存在する場合にはS23へ進み、存在しない場合にはS30へ進んでエラー通知を使用者側（コンピュータ）へ返して処理を終了する。S23では鍵管理部7が乱数発生部3に生成要求信号bを出力して乱数発生部3に鍵番号a2用の擬似乱数と暗号鍵c用の擬似乱数とを生成させる。

【0054】次いで「暗号鍵枠のループ」に入り、S24で鍵管理部7は、乱数発生部3によって生成された鍵番号a2としての擬似乱数の値を、鍵格納部4や図示しない鍵番号a2用の記憶手段に既に格納されている鍵番号a2（あるいはa2…）としての擬似乱数の値と比較

する。比較対象を暗号化記憶装置1の電源の遮断で消滅させたくない場合は、鍵番号a2用の記憶手段として不揮発性の記憶媒体をどこかに設ければよい。そして、既に記憶されている鍵番号a2（あるいはa2…）の中に生成されたばかりの鍵番号a2と一致するものがなければS25へ進み、一致するものがあればS23に戻って乱数発生部3に鍵番号a2を生成し直させる。S25では鍵管理部7は、乱数発生部3によって生成された最新の暗号鍵cを、鍵格納部4に既に記憶されている暗号鍵c（あるいはc…）と比較する。そして、鍵格納部4に既に記憶されている暗号鍵c（あるいはc…）の中に生成された最新の暗号鍵cと一致するものがなければ「暗号鍵枠のループ」を抜けてS26へ進み、一致するものがあればS23に戻って乱数発生部3に暗号鍵cを生成し直させる。このとき無効とされている暗号鍵cも比較対象とする。鍵管理部7は、一致した最新の暗号鍵cを鍵格納部4には記憶せず、自動的に使用者への割り当て対象外とする。

【0055】S26では鍵管理部7が鍵番号a2を設定して記憶させ、S27では鍵管理部7が最新の暗号鍵cを設定して鍵格納部4に記憶させる。そして、S28で鍵管理部7が鍵番号a2および最新の暗号鍵cを未使用の割り当て枠のいずれかの鍵番号a2および暗号鍵cとし、その割り当て枠のフラグを“0”から“1”に変更する。S29で鍵管理部7が、設定した鍵番号a2を使用者に返すと処理が終了する。以上が鍵付与の手順である。

【0056】〔実施の形態2〕本発明のデータ記憶装置を具現する他の実施の形態について図8ないし図15を用いて説明すれば以下の通りである。なお、前記実施の形態1で述べた構成要素と同一の機能を有する構成要素については同一の符号を付し、その説明を省略する。

【0057】図8に、本実施の形態に係るデータ記憶装置としての暗号化記憶装置11の構成を示す。暗号化記憶装置11は、実施の形態1で述べた暗号化記憶装置1にタイマー12を追加した構成である。タイマー12は、一定時間ごとに信号fを生成して鍵管理部7に入力する。鍵管理部7は信号fが入力されると生成要求信号bを乱数発生部3に入力し、乱数発生部3は生成要求信号bの入力タイミングを前記所定のタイミングとして暗号鍵cを生成する。すなわち、乱数発生部3の前記所定のタイミングはタイマー12の信号fの生成タイミングに連動している。

【0058】このようなタイマー12を備える構成における割り当て枠の構造の一例を図9に示す。鍵番号a2は0からNまであり、従って割り当て枠も同数存在し、それぞれに1つの暗号鍵cが対応する。鍵管理部7は、タイマー12が信号fを生成することに異なる割り当て枠に順に暗号鍵cを当てはめていく。タイマー12によって信号fが生成されると、次の信号fが生成されるま

では同じ暗号鍵cが最新の暗号鍵cとなり、鍵管理部7は、最新の暗号鍵cに対応する鍵番号a2を現在の鍵番号a2として認識する。そして、暗号鍵cの割り当て（「鍵付与」と称する）を図10のフローチャートを用いて説明すると、使用者側（コンピュータ）から鍵管理部7へ割り当て要求信号a1が入力されると、S41で鍵管理部7が使用者側（コンピュータ）へ現在の鍵番号a2を返す（通知する）という手順になる。鍵管理部7は、現在の鍵番号a2を順に更新して割り当て枠が一巡すると、次の更新時には初めの割り当て枠の暗号鍵cを最新の暗号鍵cに書き替えるといったように、一定時間ごとに現在の鍵番号a2の割り当て枠を継続して変更する。

【0059】図9の割り当て枠を用いる場合の、現在の鍵番号a2の設定（「鍵更新」と称する）の手順を図11のフローチャートを用いて説明する。まず、タイマー12から鍵管理部7に信号fが入力されると、S51で鍵管理部7は次の現在の鍵番号a2を計算する。S52で、鍵管理部7は計算した鍵番号a2がその時点で暗号化あるいは復号化に使用されているか否かを判定し、暗号化あるいは復号化に使用されていない場合にはS55へ進み、暗号化あるいは復号化に使用されている場合にはS53へ進んでエラー通知を使用者側（コンピュータ）へ行い、S54で使用中の鍵番号a2の使用が完了するまで待つてS55へ進む。S55では鍵管理部7が乱数発生部3に生成要求信号bを入力して暗号鍵cを生成させる。

【0060】S56では鍵管理部7が、乱数発生部3によって生成された最新の暗号鍵cとしての擬似乱数の値を、鍵格納部4に既に記憶されている暗号鍵c（あるいはc…）としての擬似乱数の値と比較する。そして、鍵格納部4に既に記憶されている暗号鍵c（あるいはc…）の中に生成された最新の暗号鍵cと一致するものがなければS57へ進み、一致するものがあればS55に戻って乱数発生部3に暗号鍵cを生成し直させる。そして鍵管理部7は、S57で最新の暗号鍵cを設定して鍵格納部4に記憶させ、S58で現在の鍵番号a2を更新し、S59で一定時間、すなわちタイマー12から次の信号fが入力されるまで待つ。次の信号fが入力されるとS51へ戻る。以上が鍵更新の手順である。

【0061】以上に述べた暗号化記憶装置11によれば、放置しておいても乱数発生部3に暗号鍵cを次々に生成させることができるので、暗号鍵cの生成のきっかけを使用者側が意図的に与える必要がない。

【0062】なお、暗号化記憶装置11において、鍵管理部7が、暗号鍵cを使用者へ割り当ててから所定時間が経過すると、鍵番号a2が入力されてもその鍵番号a2に対応する暗号鍵cを暗号化部5および復号化部6に与えないようにすることもできる。このようにすれば、割り当てから所定時間が経過すると暗号鍵cが使用不可

となるので、同じ暗号鍵cが使用者に長い間占有されるのを防止することができる。また、暗号鍵cを使用不可とする指示を使用者から与えなくても使用不可となるので、不揮発性記憶部2から暗号化データd2が不用意に読み出される可能性を自動的に極力小さくすることができる。

【0063】このように暗号鍵cを使用不可とするには、例えば暗号化記憶装置11に時計を備え、鍵番号a2の付与（暗号鍵cの割り当て）の日時を記憶しておき、記憶した日時から所定時間が経過したときに鍵管理部7が割り当て枠の該当する暗号鍵cを無効にすることで実現することができる。なお、このような構成は実施の形態1で述べた暗号化記憶装置1や、後述する暗号化記憶装置21にも適用することができる。

【0064】上記時計を備えた構成の場合の、割り当て枠の構造の一例を図12に示す。0からNまでの鍵番号a2の各割り当て枠に、暗号鍵cと対で、暗号鍵cの割り当て日時（必要に応じて年月）が鍵番号a2の使用開始日時を示す情報として記憶される。使用開始日時から所定時間が経過した鍵番号a2の割り当て枠には、鍵管理部7によって使用開始日時の情報が消去されてフラグ“0”に変更（リセット）される。

【0065】図12の割り当て枠を用いる場合の、暗号鍵cの無効化（「鍵強制解放」と称する）の手順を図13のフローチャートに示す。まず「暗号鍵枠のループ」に入り、S61で鍵管理部7が鍵番号a2の付与（暗号鍵cの割り当て）から所定時間が経過したか否かを判定し、経過していればS62へ進み、経過していなければ「暗号鍵枠のループ」を抜けてS66へ進む。S62では鍵管理部7が、所定時間が経過した鍵番号a2（暗号鍵c）がその時点で暗号化あるいは復号化に使用されているか否かを判定し、暗号化あるいは復号化に使用されていないとS65へ進む。一方、暗号化あるいは復号化に使用されているとS63で使用者側（コンピュータ）にエラー通知を行い、S64で使用中の鍵番号a2（暗号鍵c）の使用が完了するまで待つてS65へ進む。S65では鍵管理部7が該当する鍵番号a2の割り当て枠の使用開始日時の情報をフラグ“0”に変更（リセット）する。これで「暗号鍵枠のループ」を抜け、S66で前記所定時間が経過するまで待つてS61に戻る。以上が鍵強制解放の手順である。

【0066】次に、図14に、前記暗号化記憶装置11の変形例である暗号化記憶装置（データ記憶装置）21の構成を示す。暗号化記憶装置21は、暗号化記憶装置11にセクタ22・23を追加した構成である。セクタ22は暗号化記憶装置21のデータd1の入力側と暗号化部5および復号化部6との間に設けられる。セクタ23は暗号化部5および復号化部6と不揮発性記憶部2との間に設けられる。セクタ22・23には、暗号化の要否を示す暗号化要否信号gと、復号化の要否を示

す復号化要否信号hとが使用者側(コンピュータ)から入力されるようになっている。

【0067】データd1の暗号化を行う際には、セレクト22・23に暗号化を要求することを示す暗号化要否信号gが入力され、セレクト22は暗号化記憶装置21に入力されるデータd1が暗号化部5に入力されるように経路を切り替え、セレクト23は暗号化部5から出力される暗号化データd2が不揮発性記憶部2に入力されるように経路を切り替える。データd2の復号化を行う際には、セレクト22・23に復号化を要求することを示す復号化要否信号hが入力され、セレクト23は不揮発性記憶部2から出力される暗号化データd2が復号化部6に入力されるように経路を切り替え、セレクト22は復号化部6から出力される復号データd3が暗号化記憶装置21から使用者側(コンピュータ)に出力されるように経路を切り替える。

【0068】また、暗号化を行わないデータd1については、不揮発性記憶部2への記憶の際に、セレクト22・23に暗号化を要求しないことを示す暗号化要否信号gが入力され、セレクト22・23は、データd1がセレクト22から直接セレクト23に渡されて不揮発性記憶部2へ入力されるように経路を切り替える。また、この暗号化しなかったデータd1を不揮発性記憶部2から読み出す際には、セレクト22・23に復号化を要求しないことを示す復号化要否信号hが入力され、セレクト22・23は、データd1がセレクト23から直接セレクト22に渡されて暗号化記憶装置21から使用者側(コンピュータ)に出力されるように経路を切り替える。

【0069】上記暗号化記憶装置21を用いたデータの読み書きの手順を、図15のフローチャートを用いて説明する。まずS71で鍵管理部7はデータ読み書きの処理中であるか否かを判定し、データ読み書きの処理中でなければS72に進む。一方、データ読み書きの処理中であればS79へ進んで使用者にビジー通知を行って処理を終了する。S72で鍵管理部7はデータの暗号化あるいは復号化を行うか否かを判定し、データの暗号化あるいは復号化を行う場合にはS73へ進む。一方、データの暗号化あるいは復号化を行わない場合にはS77へ進んで暗号化を要求しないことを示す暗号化要否信号g、あるいは復号化を要求しないことを示す復号化要否信号hをセレクト22・23に入力してセレクト22とセレクト23とが直接つながるように経路を切り替え、S78へ進む。

【0070】S73では鍵管理部7が使用者側(コンピュータ)から鍵番号a2を受け取り、S74で鍵管理部7が対応する暗号鍵cを鍵格納部4から検索して読み出す。S75では鍵管理部7が暗号化部5あるいは復号化部6に暗号鍵cを与える(セットする)。S76では暗号化を要求することを示す暗号化要否信号g、あるいは

復号化を要求することを示す復号化要否信号hをセレクト22・23に入力して、セレクト22・23に暗号化用あるいは復号化用の経路に切り替えさせる。そして、S78でデータの読み書きを行って処理を終了する。

【0071】このように、暗号化記憶装置21によれば、セレクト22・23が設けられているので、暗号化および復号化しないデータをも不揮発性記憶部2に記憶させることができる。

【0072】

【発明の効果】本発明のデータ記憶装置は、以上のように、所定のタイミングで擬似乱数を生成し、上記タイミングごとの擬似乱数を暗号鍵とする暗号鍵発生手段と、上記暗号鍵発生手段によって生成された上記暗号鍵を記憶する記憶データ揮発性の暗号鍵記憶手段と、上記暗号鍵が与えられると、入力されるデータを上記暗号鍵によって暗号化して上記不揮発性記憶手段に暗号化データとして記憶させる暗号化手段と、暗号化の際と同一の上記暗号鍵が与えられると、上記不揮発性記憶手段に記憶されている上記暗号化データを上記暗号鍵によって復号化して読み出す復号化手段と、外部から行われる使用者への上記暗号鍵の割り当て要求に対して上記割り当て要求時に最新の上記暗号鍵に対応する暗号鍵情報を返し、入力されるデータを暗号化する指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記暗号化手段に与え、上記暗号化データを読み出す指示および上記暗号鍵情報が入力されると上記暗号鍵情報に対応する上記暗号鍵を上記暗号鍵記憶手段から読み出して上記復号化手段に与える暗号鍵管理手段と、を備えている構成である。

【0073】それゆえ、生成された最新の暗号鍵を使用者に割り当てることにより、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を高い確率で異ならせることができる。これにより、様々な暗号鍵によるデータの暗号化および復号化を容易に行うことができるようになり、不揮発性記憶手段には暗号鍵の異なる複数の暗号化データを記憶させることができる。

【0074】また、暗号鍵記憶手段は記憶データ揮発性であるので、持ち出されるなどしてデータが解析される場合には、通常電源が遮断されて暗号鍵記憶手段に記憶されていた暗号鍵は消滅する。この状態で不揮発性記憶手段に記憶されている暗号化データを解析された場合、解析が容易な暗号化データが偶然存在してこの暗号化データの暗号鍵が推測されたとしても、推測された暗号鍵では、その他の異なる暗号鍵で暗号化された暗号化データを復号化することはできない。また、持ち出された不揮発性記憶手段の暗号化データについての暗号鍵が推測されたとしても、今後この不揮発性記憶手段に記憶される暗号化データの暗号鍵には擬似乱数が使用されるので、推測されたものとは異なる確率が非常に高い。従って、暗号化データが使用者以外に連鎖的に判別されるこ

とはほとんどない。

【0075】この結果、非関係者に不揮発性の記憶媒体の記憶データが連鎖的に判別されるのを抑制することのできるデータ記憶装置を提供することができるという効果を奏する。

【0076】また、使用者が暗号化データをこれ以上読み出す必要がなくなった場合に、上述したように非関係者による暗号鍵の推測は、解析が容易なデータでない限り困難である。従って、不揮発性記憶手段に記憶されている暗号化データを消去するといった、データ入出力の妨げとなる時間のかかる作業は不要である。この結果、読み出す必要がなくなった不揮発性の記憶媒体の記憶データを、データ入出力の効率を低下させることなく非関係者に読み出し困難とすることのできるデータ記憶装置を提供することができるという効果を奏する。

【0077】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵発生手段は、外部からの上記暗号鍵の生成要求を受け付け、上記生成要求時を上記所定のタイミングとして上記暗号鍵を生成する構成である。

【0078】それゆえ、暗号鍵を生成したいときに暗号鍵発生手段に暗号鍵を生成させるので、既に生成されて暗号鍵記憶手段に記憶されている暗号鍵とは異なる暗号鍵を容易に得ることができるという効果を奏する。また、無駄な暗号鍵の生成を避けることができるという効果を奏する。

【0079】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、上記割り当て要求時に上記暗号鍵発生手段に上記生成要求を行う構成である。

【0080】それゆえ、割り当て要求ごとに異なる暗号鍵を容易に得ることができる。従って、データを他の使用者に判別されにくいものとしたり、同一使用者の読み出し対象としていないデータが読み出されてしまうことを避けたりすることができるという効果を奏する。また、暗号鍵の生成要求を別途行わなくてもすむという効果を奏する。

【0081】さらに本発明のデータ記憶装置は、以上のように、一定時間ごとに信号を生成するタイマーを備え、上記暗号鍵発生手段の上記所定のタイミングが上記信号の生成タイミングに連動している構成である。

【0082】それゆえ、放置しておいても暗号鍵発生手段に暗号鍵を次々に生成させることができるので、暗号鍵の生成のきっかけを意図的に与える必要がないという効果を奏する。

【0083】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵記憶手段に複数の上記暗号鍵が記憶される構成である。

【0084】それゆえ、暗号鍵のそれぞれを別々のデータの暗号化および復号化に用いることができるので、同じ期間に異なる使用者に異なる暗号鍵を割り当てたり、同一使用者に異なるデータの処理用に異なる暗号鍵を割

り当てたりすることができる。従って、同じ期間に各データの機密保持が確保された状態での不揮発性記憶手段の使用可能回数が増加し、データの暗号化および復号化の効率を向上させることができるという効果を奏する。

【0085】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、上記暗号鍵発生手段によって生成された最新の上記暗号鍵を上記暗号鍵記憶手段に既に記憶されている上記暗号鍵と比較して一致するものがある場合には、上記暗号鍵発生手段に最新の上記暗号鍵を一致しなくなるまで生成し直させ、一致する上記暗号鍵は使用者に割り当てない構成である。

【0086】それゆえ、暗号鍵記憶手段に既に記憶されている暗号鍵とは異なる最新の暗号鍵が使用者に割り当てられるので、擬似乱数の異なる生成タイミングを経て割り当てられる複数の暗号鍵を確実に異ならせることができるという効果を奏する。

【0087】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、外部から上記暗号鍵を無効にする指示を上記暗号鍵に対応する上記暗号鍵情報との組合せで受け付けて、上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えないようにする構成である。

【0088】それゆえ、暗号鍵をもう使用しないときにいつでも暗号鍵をデータの暗号化や復号化に使用不可とすることができるので、データが不用意に読み出される可能性を極力小さくすることができるという効果を奏する。

【0089】さらに本発明のデータ記憶装置は、以上のように、上記暗号鍵管理手段は、上記暗号鍵の使用者への割り当てから所定時間が経過すると上記暗号鍵情報が入力されても上記暗号鍵を上記暗号化手段および上記復号化手段に与えない構成である。

【0090】それゆえ、割り当てから所定時間が経過すると暗号鍵が使用不可となるので、同じ暗号鍵が使用者に長い間占有されるのを防止することができるという効果を奏する。また、暗号鍵を使用不可とする指示を使用者から与えなくても使用不可となるので、データが不用意に読み出される可能性を自動的に極力小さくすることができるという効果を奏する。

【0091】さらに本発明のデータ記憶装置は、以上のように、擬似乱数を上記暗号鍵情報として生成する暗号鍵情報発生手段を備えている構成である。

【0092】それゆえ、暗号鍵情報が擬似乱数で使用者に与えられるので、過去に与えられた暗号鍵情報を使用したデータの不正な暗号化および復号化が行われるのを防止することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係るデータ記憶装置の構成を示すブロック図である。

【図2】(a) および (b) は、図1のデータ記憶装置

の暗号化部および復号化部の構成を示す回路ブロック図である。

【図3】図1のデータ記憶装置に用いられる割り当て枠の構造例を説明する説明図である。

【図4】図3の割り当て枠を用いた場合の鍵付与の手順を示すフローチャートである。

【図5】図3の割り当て枠を用いた場合の鍵解放の手順を示すフローチャートである。

【図6】図1のデータ記憶装置に用いられる割り当て枠の他の構造例を説明する説明図である。

【図7】図6の割り当て枠を用いた場合の鍵付与の手順を示すフローチャートである。

【図8】本発明の他の実施の形態に係るデータ記憶装置の構成を示すブロック図である。

【図9】図8のデータ記憶装置に用いられる割り当て枠の構造例を説明する説明図である。

【図10】図9の割り当て枠を用いた場合の鍵付与の手順を示すフローチャートである。

【図11】図9の割り当て枠を用いた場合の鍵更新の手順を示すフローチャートである。

【図12】図8のデータ記憶装置に用いられる割り当て枠の他の構造例を説明する説明図である。

【図13】図12の割り当て枠を用いた場合の鍵強制解

放の手順を示すフローチャートである。

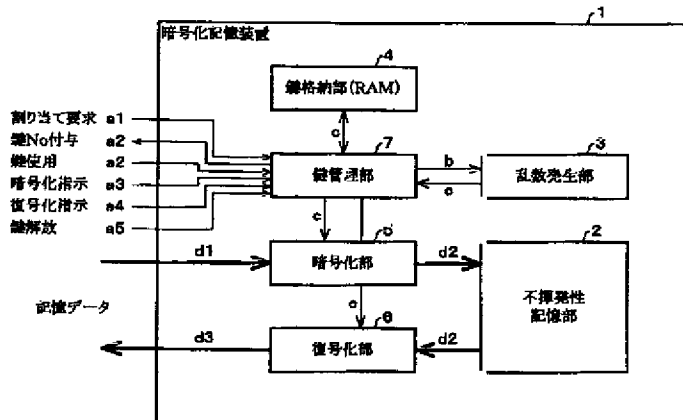
【図14】本発明の他の実施の形態に係るデータ記憶装置の変形例の構成を示すブロック図である。

【図15】図14のデータ記憶装置を用いた場合のデータの読み書きの手順を示すフローチャートである。

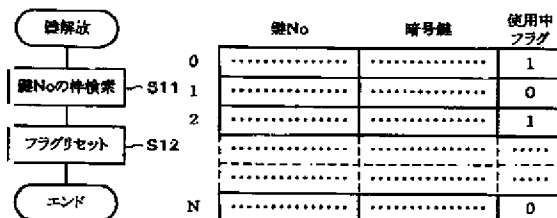
【符号の説明】

- 1 暗号化記憶装置（データ記憶装置）
- 2 不揮発性記憶部（不揮発性記憶手段）
- 3 乱数発生部（暗号鍵発生手段、暗号鍵情報発生手段）
- 4 鍵格納部（暗号鍵記憶手段）
- 5 暗号化部（暗号化手段）
- 6 復号化部（復号化手段）
- 7 鍵管理部（暗号鍵管理手段）
- 11 暗号化記憶装置（データ記憶装置）
- 12 タイマー
- 21 暗号化記憶装置（データ記憶装置）
- a2 鍵番号（暗号鍵情報）
- c 暗号鍵
- d1 データ
- d2 暗号化データ
- f 信号

【図1】



【図5】



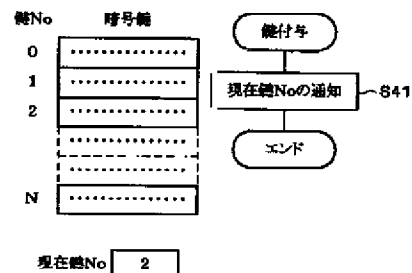
【図6】

【図3】

鍵No	暗号鍵	使用中 フラグ
0	1
1	0
2	1
...
N	0

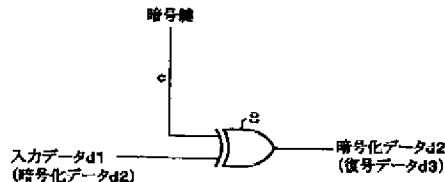
【図9】

【図10】

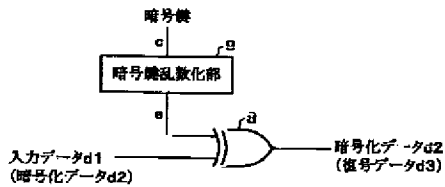


【図2】

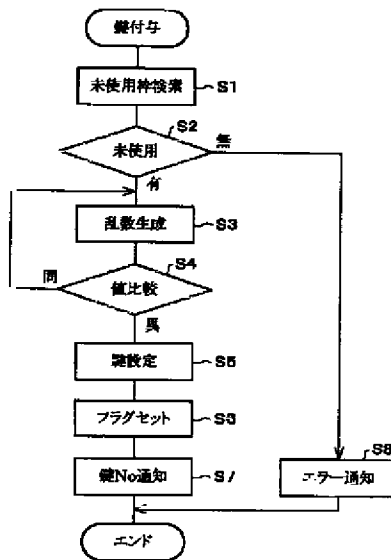
(a)



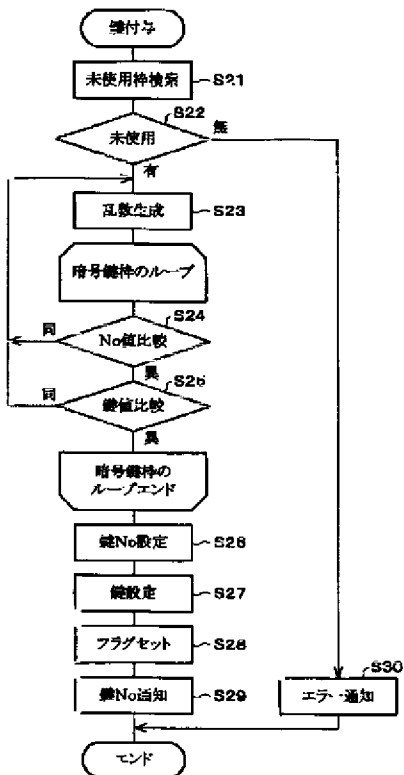
(b)



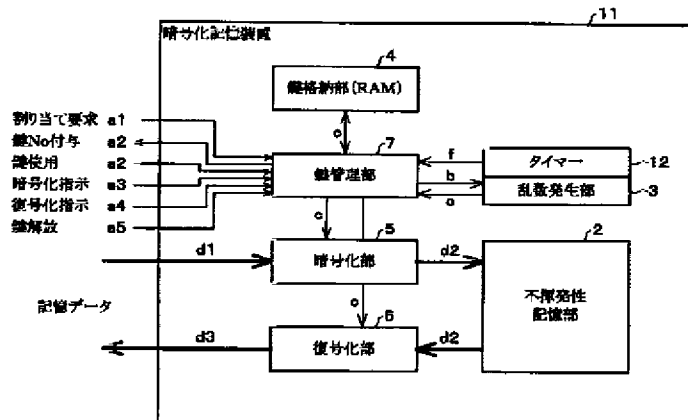
【図4】



【図7】



【図8】

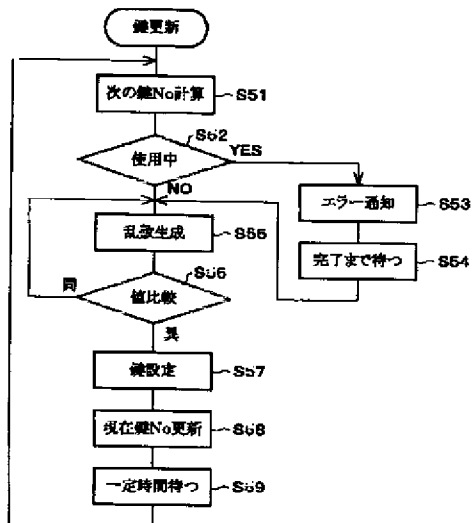


【図12】

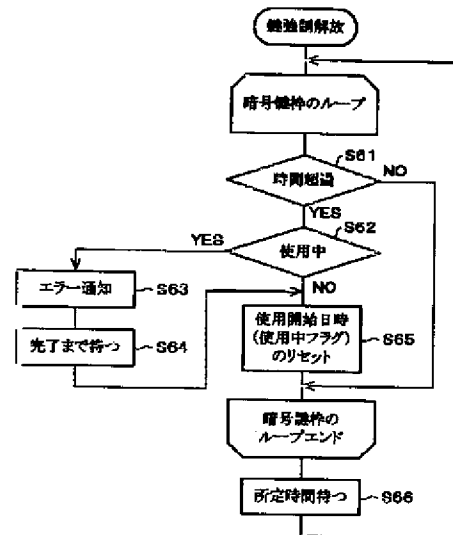
鍵No	暗号鍵	使用開始日時
0	200012150820
1	0
2	200012141557

N	0

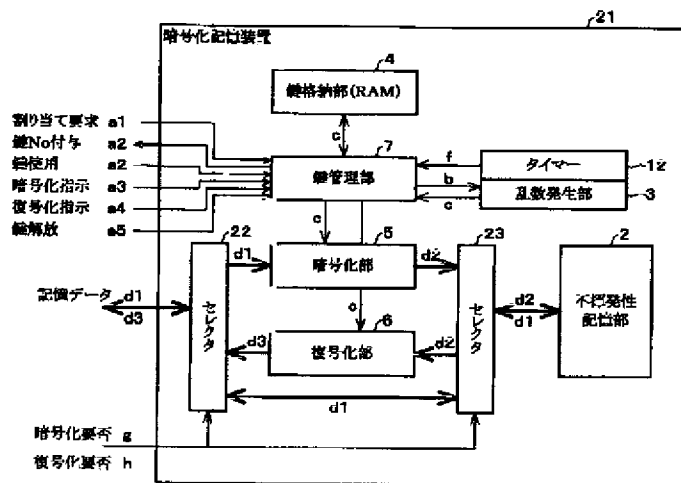
【図11】



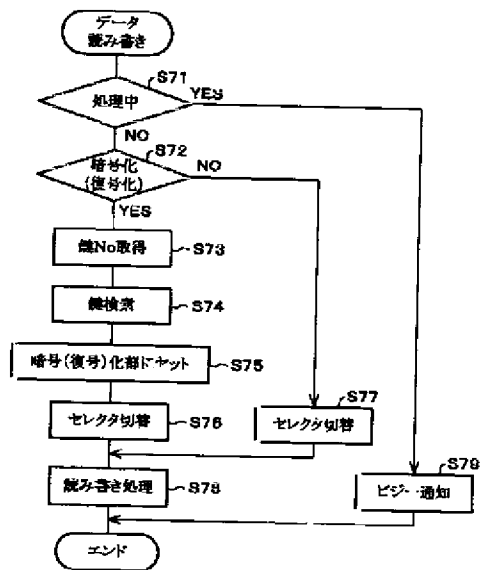
【図13】



【図14】



【図15】



フロントページの続き

Fターム(参考) 5B017 AA07 BA07 CA16
5D044 AB01 BC01 BC04 CC04 DE49
EF05 GK12 GK17 HH15
5D110 AA13 DB05 DB11 DC03 DC19
DC22 DC27 DD13